Internal Control Evaluation
Risk Assessment Tool

Objective of the Risk Assessment Tool

The objectives of this risk assessment tool are to:

1. Provide quantifiable criteria for assessing risk throughout the department, resulting in the identification of activities or programs that are critical to the department in achieving its overall mission and meeting department-wide goals and objectives.
2. To assist in building an inventory of the information technology (IT) applications by identifying specific applications that support the activities or programs.

Overview

An activity or program may be defined as one or several organizational components that seek to achieve common business objectives. Alternatively, the activity may correlate with a core business process that "cuts across" multiple activities (e.g. administrative activities, human resources, and information technology). Successfully assessing risk at an activity or program level contributes to maintaining acceptable levels of risk at the department wide level. Identifying and analyzing risks is a continuous process critical to maintaining effective internal control.

A prerequisite to conducting a risk assessment is establishing objectives, linked at different levels (department wide and activity or program level) and internally consistent. Risk assessment is the identification and analysis of relevant risks to the achievement of the objectives, forming a basis for determining how to mitigate and/or manage the risks.

The risk assessment tool should be applied to all department activities or programs as a mechanism for determining the degree of risk each activity or program present to the department as a whole.

Completing the Risk Assessment

Prior to conducting activity level risk assessments, the Internal Control Officer (ICO) should evaluate the risk categories and criteria provided on the risk assessment tool. The ICO has the discretion to add, remove, or modify the risk categories, or the order, as necessary, based on the organizational structure and the nature of department's activities or programs.

For each activity or program, the manager should identify the IT application(s) that provide support to the activity or program.

Analyzing the Results of the Assessment

The ICO should develop ranges for the overall scores that translates the results into "high," "medium," or "low," risk classifications. At a minimum, the department should conduct comprehensive evaluation and monitoring efforts for all "high" risk activities or programs, and as many of the "medium" and "low" risk activities or programs as possible, if resources are not sufficient to include all of them. The "medium" and "low" risk activities or programs not included in the comprehensive evaluation and monitoring efforts should have their control systems documented, with more extensive evaluations conducted as frequently as possible to allow those activities or program level managers to have reasonable assurance about the ongoing effectiveness of the internal control system of their activity or program.

While analyzing the results of the risk assessments, the ICO may find it appropriate to adjust the activity or program level scoring to ensure the criteria was consistency applied throughout the department and that the judgment of the activity or program level managers is consistent with that of the ICO in regard to the activities' or programs' impact on the department wide mission, goals, and objectives.

Description of Risk Categories

Importance of the Activity to the Department Mission/Objectives – management's ranking of the importance of the activity to the department and its mission/objectives. Used to rate the reliance management places on the activity or program to help fulfill the department's mission and attain its corresponding goals and objectives.

Regulatory/Legal Requirements – the level of regulatory or legal requirements the activity is subject to. Used to rate the risk associated with non-compliance with the regulatory or legal requirements.

Sensitive/Confidential Information – the level of sensitive or confidential information contained or processed through the activity. Used to rate the risk associated with disclosure of such information by the activity.

Control Environment – the knowledge of internal control within the activity or program and the attitude of management toward internal control. Used to rate the risk associated with internal controls by those that uses/performs the activity.

Federal Funding – whether or not the activity is federally funded. Used to rate the risk associated with statutory review of activities under federal regulations.

Dollars Supported – the total costs associated with the activity in one fiscal year. Dollars should be estimated if not known. The greater the dollars, the greater the potential dollar impact of errors.

Outside Reliance – the degree to which outside users rely on information received from the activity. Used to rate the risk associated with user dependence on accurate information processed by the activity.

Volume of Transactions/Program Activities – a judgmental determination of the volume of transactions processed in one year and/or the level of program activities. Used to rate the risk associated with the volume of transactions and level of activities; the more transactions and higher the level of activities the greater the reliance on the activity and the risk errors occur undetected.

Prior Audit/Fraud Occurrences – the number of times, or frequency, that fraud has been recorded or reported in the past regarding the activity. Used to rate the risk of future fraud.

Decentralization/Number of Program Staff – the degree to which activities are decentralized, combined with the number of staff involved with carrying out the activities. Decentralization refers to the number, location, and classification of personnel using/providing the activity. Used to rate the risk associated with additional locations and multiple staff or users and degree of internal control.

Program Staff Training – the level of training required for staff to properly learn duties of the activity. Used to rate the knowledge and competency of users based on hands on training with the function.